The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

9/18/2014

SUBJECT:

Multiple Vulnerabilities in Apple Mac OS X Prior to 10.9.5

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Apple's Mac OS X prior to 10.9.5. Mac OS X is an operating system for Apple computers. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of OS X. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and bypass of security systems.

THREAT INTELLIGENCE

There is no known proof-of-concept code available at this time.

SYSTEM AFFECTED:

- Apple OS X prior to 10.9.5

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Apple Mac OS X. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file. The vulnerabilities are as follows:

- A local security-bypass vulnerability in the kernel. Specifically, this issue occurs because CPU Global Descriptor Table is allocated at a predictable address (CVE-2014-4403).
- An arbitrary code-execution vulnerability because it fails to properly validate user-supplied input. Specifically, this issue occurs due to a null-pointer-deference condition with in the IOAcceleratorFamily component when handling IOKit API arguments (CVE-2014-4376).
- An arbitrary code-execution vulnerability because it fails to properly bounds check user-supplied input. Specifically, this issue occurs in the Intel Graphics Driver (CVE-2014-4394, CVE-2014-4396, CVE-2014-4395, CVE-2014-4397, CVE-2014-4398, CVE-2014-4399, CVE-2014-4400, CVE-2014-4401, CVE-2014-4416).
- An arbitrary code-execution vulnerability because it fails to properly bounds check user-supplied input. Specifically, this issue occurs because the application fails to properly handle a Bluetooth API call (CVE-2014-4390).
- An integer-overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data. Specifically, the issue occurs in the 'CoreGraphics' component when handling specially crafted PDF files (CVE-2014-4377).
- A buffer-overflow vulnerability because it fails to perform adequate bounds checks on user-supplied input. Specifically, this issue exists in the handling of a crafted MIDI file of the 'QT Media Foundation' component (CVE-2014-4350).
- An information-disclosure vulnerability because it fails to properly handle external XML data. Specifically, this issue occurs in the NSXMLParser of the Foundation module (CVE-2014-4374).

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to affected systems immediately after appropriate testing.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download or open files from un-trusted websites, unknown users, or suspicious emails.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Adobe:

http://support.apple.com/kb/HT6443

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4350
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4376

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4377

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4390

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4394

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4395

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4396

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4397

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4398

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4399

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4400

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4401

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4403

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4416